



PCT/FR00/00172

ESU

REC'D 04 FEB 2000
WIPO PCT

~~FR00/172~~

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

14 JAN. 2000

Fait à Paris, le

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITE

PRESENTÉ OU TRANSMIS
CONFORMEMENT A LA REGLE
17.1.a) OU b)

Martine PLANCHE

SIEGE
INSTITUT
NATIONAL DE
LA PROPRIETE
INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS Cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

REQUÊTE EN DÉPÔT

Confirmation d'un dépôt par télécopie

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

01 FEV 1999

N° D'ENREGISTREMENT NATIONAL

99 01096 -

DÉPARTEMENT DE DÉPÔT

TS

01 FEV. 1999

2 DEMANDE Nature du titre de propriété industrielle

- brevet d'invention demande divisionnaire
 certificat d'utilité transformation d'une demande de brevet européen.



demande initiale

brevet d'invention

Établissement du rapport de recherche

- différé immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

n°du pouvoir permanent références du correspondant téléphone

MF-BFF980238 01 44 63 4111

date

Titre de l'invention (200 caractères maximum)

PROCEDE ET SYSTEME DE CONTROLE D'ACCES A UNE RESSOURCE LIMITE A CERTAINES PLAGES HORAIRES, LES RESSOURCES ACCEDANTE ET ACCEDEE ETANT DEPOURVUES D'HORLOGE TEMPS REEL.

3 DEMANDEUR (S) n° SIREN

code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

Forme juridique

FRANCE TELECOM

SOCIETE ANONYME

Nationalité (s) FRANCAISE

Adresse (s) complète (s)

Pays

6, PLACE D'ALLERAY
75015 PARIS

France.

En cas d'insuffisance de place, poursuivre sur papier libre 4 INVENTEUR (S) Les inventeurs sont les demandeurs oui non Si la réponse est non, fournir une désignation séparée5 RÉDUCTION DU TAUX DES REDEVANCES requise pour la 1ère fois requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire)

CABINET PLASSERAUD

Michel FRECHEDÉ (CPI N°92-1093).

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

*Frechedé**[Signature]*

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

9901096

MF / EMA-BFF980238

TITRE DE L'INVENTION :

PROCEDE ET SYSTEME DE CONTROLE D'ACCES A UNE RESSOURCE LIMITE
A CERTAINES PLAGES HORAIRES, LES RESSOURCES ACCEDANTE ET ACCEDEEE
ETANT DEPOURVUES D'HORLOGE TEMPS REEL.

Le titulaire, FRANCE TELECOM,
ayant pour mandataire

LE(S) SOUSSIGNÉ(S)

CABINET PLASSERAUD
84, RUE D'AMSTERDAM
75440 PARIS CEDEX 09

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

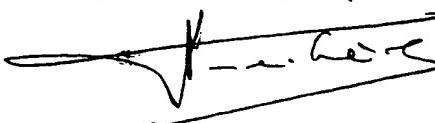
1. CLERC Fabrice
33, avenue Robert Schuman
14000 CAEN
FRANCE.
2. GIRAUT Marc
9, rue Bernard Vanier
14000 CAEN
FRANCE.

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Paris,
Le 01.02.1999.

CABINET PLASSERAUD
Michel FRECHEDE (CPI N°92-1093)



PROCÉDÉ ET SYSTÈME DE CONTRÔLE D'ACCÈS À UNE RESSOURCE
LIMITÉ À CERTAINES PLAGES HORAIRES, LES RESSOURCES ACCÉDANTE
ET ACCÉDÉE ÉTANT DÉPOURVUES D'HORLOGE TEMPS RÉEL

5 La présente invention concerne un procédé et un système de contrôle d'accès, par une ressource accédante ou clé électronique, dépourvue d'horloge temps réel, à une ressource accédée ou serrure électronique, également dépourvue d'horloge temps réel, cet accès étant limité à
10 certaines plages horaires.

Elle s'applique au contrôle d'accès à une ressource quelconque, ressource accédée, dont on souhaite contrôler l'utilisation, et dont on souhaite limiter l'accès à une ou plusieurs plages horaires déterminées, dites aussi plages de validité prédéterminées, que la ressource considérée soit un bâtiment, un système informatique, ou tout autre objet, tel qu'une boîte aux lettres ou un coffre de banque.

20 L'invention s'applique plus particulièrement au contrôle d'accès à des ressources accédées non autonomes en énergie et/ou ne disposant que d'un potentiel limité de vérification d'une plage horaire de validité, notamment les ressources ne disposant pas d'horloge temps réel.

25 La plage de validité peut être, soit la période proprement dite pendant laquelle il est possible d'accéder à la ressource, soit tout autre paramètre permettant de limiter dans le temps une attaque par utilisation frauduleuse de la ressource accédante.

30 Le principal avantage d'un moyen d'accès logique à une ressource par rapport à un moyen d'accès physique réside généralement dans la possibilité de ne permettre l'accès à la ressource qu'à l'intérieur d'une plage horaire relativement courte prédéterminée.

Dans ces conditions, si la clé électronique est perdue, volée, cédée ou dupliquée, elle ne permettra pas à son détenteur illégitime d'accéder à la ressource en dehors de la plage horaire prédéterminée. Cela suppose cependant 5 que la ressource accédée soit en mesure de vérifier que cette plage horaire est respectée. Cela implique généralement que la ressource accédée dispose d'une horloge temps réel.

Ainsi, le document FR-A-2 722 596 décrit un système de 10 contrôle d'accès limités à des plages horaires autorisées et renouvelables au moyen d'un support de mémorisation portable. Ce système, fondé sur des mécanismes cryptographiques, permet de limiter la période de validité 15 des droits d'accès à une courte durée, afin d'éviter une utilisation illégitime en cas de perte, vol, cession ou duplication illicites.

Toutefois, la solution décrite repose sur l'hypothèse, 20 fortement contraignante, que la ressource accédée soit autonome en énergie, pour maintenir une horloge temps réel lui permettant de vérifier la validité de la plage horaire dans laquelle a lieu la tentative d'accès par la ressource accédante.

On connaît également des procédés et systèmes de 25 contrôle d'accès dans lesquels la ressource accédée ne comporte pas d'horloge temps réel, mais uniquement un compteur, remis à jour après une tentative d'accès réussie de la ressource accédante à la ressource accédée.

Toutefois, dans de tels procédés et systèmes, la 30 remise à jour du compteur, dans la ressource accédée, est généralement effectuée par la ressource accédante, au moyen d'une horloge temps réel dont est munie la ressource accédante.

Un inconveniant de cette solution est qu'elle impose d'assurer l'autonomie en énergie de la ressource accédante, afin que cette dernière puisse maintenir en permanence son horloge temps réel.

5 La présente invention a pour but de remédier aux inconvenients précités en permettant à une ressource accédée de vérifier une plage de validité associée à un droit d'accès présenté par une ressource accédante tout en supprimant la nécessité de présence d'une horloge temps
10 10 réel, non seulement dans la ressource accédée, mais également dans la ressource accédante.

Dans ce but, la présente invention propose un procédé de contrôle d'accès d'au moins une clé électronique à au moins une serrure électronique, à l'intérieur d'une plage
15 15 horaire prédéterminée, suivant lequel :

(a) préalablement à toute tentative d'accès de la clé électronique à une serrure électronique, on mémorise dans la serrure une valeur horaire de contrôle, délivrée par une horloge temps réel d'une entité de validation
20 20 extérieure ;

puis, lors de chaque tentative d'accès de la clé électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire prédéterminée,
25 25 préalablement mémorisée dans la clé électronique ;

(c) on mémorise dans la clé une valeur horaire d'essai, délivrée par l'horloge temps réel de l'entité de validation extérieure ;

(d) on transmet de la clé électronique à la serrure
30 30 électronique la plage horaire et la valeur horaire d'essai, et

dans la serrure électronique :

(e) on vérifie que la valeur horaire d'essai transmise est à l'intérieur de la plage horaire prédéterminée, et qu'elle est postérieure à la valeur horaire de contrôle mémorisée dans la serrure ;

5 (f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur horaire de contrôle, à partir de la valeur horaire d'essai transmise ;

10 (g) si la valeur horaire d'essai transmise est à l'extérieur de la plage horaire prédéterminée, ou si elle est antérieure à la valeur horaire de contrôle mémorisée dans la serrure, on interdit l'accès de cette clé à cette serrure.

Dans un mode de réalisation qui procure une sécurité accrue, on effectue les étapes supplémentaires ci-après :

dans la clé électronique :

20 (b1) à l'étape (b), on lit, en plus de la plage horaire, ou en lieu et place de la plage horaire, une signature électronique de cette plage horaire, préalablement calculée et mémorisée dans la clé électronique ;

(d1) à l'étape (d), on transmet de la clé électronique à la serrure électronique, d'une part, ladite signature électronique en plus ou en lieu et place de la plage horaire et, d'autre part, de la valeur horaire d'essai, et

dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature transmise, à partir d'une clé de vérification spécifique ;

30 (f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur horaire de contrôle, à partir de la valeur horaire d'essai transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

(g1) à l'étape (g), on interdit l'accès de la clé à la serrure si la valeur horaire d'essai transmise est à l'extérieur de la plage horaire, ou si elle est antérieure à la valeur horaire de contrôle mémorisée dans la serrure, ou 5 si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

En variante, l'ordre d'exécution des étapes (e1) et (e) peut être interverti.

La clé de vérification spécifique utilisée à l'étape 10 (e1) peut être une clé publique ou secrète.

Dans un autre mode particulier de réalisation susceptible de procurer une sécurité accrue, on effectue les étapes supplémentaires ci-après :

dans la clé électronique :

15 (c2) à l'étape (c), on calcule et on mémorise, en plus de la valeur horaire d'essai, une signature électronique de cette valeur horaire d'essai ;

20 (d2) à l'étape (d1), on transmet en outre, de la clé électronique à la serrure électronique, la signature électronique de la valeur horaire d'essai, et

dans la serrure électronique :

(e2) avant ou après l'étape (e), on vérifie la signature de la valeur d'essai, à partir d'une seconde clé de vérification spécifique publique ou secrète ;

25 (f2) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur horaire de contrôle, que si les vérifications effectuées aux étapes (e), (e1) et (e2) sont satisfaites ;

30 (g2) à l'étape (g), on interdit l'accès de la clé électronique à la serrure électronique si l'une des vérifications effectuées aux étapes (e), (e1) ou (e2) n'est pas satisfaites.

L'introduction d'une signature électronique de la valeur d'essai vise à prémunir la clé et la serrure électroniques contre un type de fraude qui consisterait, pour un pirate disposant d'une valeur de plage horaire et d'une valeur horaire d'essai authentiques, à modifier la valeur horaire d'essai de telle façon qu'elle devienne postérieure à la valeur horaire de contrôle contenue dans la serrure tout en restant à l'intérieur de la plage de validité.

La plage horaire précitée peut comprendre plusieurs plages horaires disjointes.

Dans un mode particulier de réalisation, la plage horaire est un intervalle comportant deux bornes exprimées chacune comme une date en jour, mois, année et un horaire en heures, minutes, secondes.

La présente invention propose également un système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique et au moins une clé électronique, dans lequel la clé comprend :

- un module de mémorisation d'une valeur horaire d'essai, accessible en lecture et en écriture, et
- un module de communication pour transmettre à la serrure une plage horaire prédéterminée et la valeur horaire d'essai, et dans lequel

la serrure comprend :

- un module de mémorisation d'une valeur horaire de contrôle, accessible en lecture et en écriture, et
- un module de comparaison de la valeur horaire d'essai à la plage horaire prédéterminée et à la valeur horaire de contrôle mémorisée dans le module de mémorisation de la serrure.

Dans un mode de réalisation qui procure une sécurité accrue, le module de communication pour transmettre à la serrure une plage horaire prédéterminée et la valeur horaire d'essai s'accompagne d'un module de transmission à la serrure d'une signature électronique de la plage horaire et d'une signature électronique de la valeur horaire d'essai, et la serrure comprend en outre un module de vérification des signatures électroniques transmises par la clé.

Dans un mode particulier de réalisation, le module de mémorisation comprend une mémoire non volatile reprogrammable électriquement.

Dans un mode particulier de réalisation, la clé électronique communique avec la serrure électronique à l'aide d'un module de transmission sans contact, par induction électromagnétique.

Ce module de transmission sans contact peut comprendre un premier bobinage électromagnétique prévu dans la clé et un second bobinage électromagnétique prévu dans la serrure.

Ces deux bobinages peuvent être concentriques.

La présente invention propose également une clé électronique comportant au moins une unité logique de calcul de clé, un module d'émission - réception de signaux de contrôle d'accès de clé pour la mise en œuvre d'un procédé de contrôle d'accès entre cette clé électronique et une serrure électronique à partir de signaux de contrôle d'accès de serrure engendrés par cette serrure électronique, cette clé étant remarquable en ce qu'elle comporte en outre :

- un module générateur d'un signal de puissance, piloté par l'unité de calcul de clé précitée ; et
- un module de transfert de clé pour transférer des signaux de contrôle d'accès de clé et de serrure et un signal de puissance, le module de transfert de clé

comportant au moins un enroulement interconnecté au module générateur d'un signal de puissance et au module d'émission - réception.

La présente invention propose en outre une serrure électronique comportant au moins une unité logique de calcul de serrure et un module d'émission - réception de signaux de contrôle d'accès de serrure pour la mise en œuvre d'un procédé de contrôle d'accès entre cette serrure électronique et une clé électronique à partir de signaux de contrôle d'accès de clé et d'un signal de puissance engendrés par cette clé électronique, cette serrure étant remarquable en ce qu'elle comporte en outre :

- un module de transfert de serrure des signaux de contrôle d'accès de clé et de serrure et du signal de puissance, le module de transfert de serrure comportant au moins un enroulement interconnecté au module d'émission - réception de signaux de contrôle d'accès de serrure ; et

- un module de stockage de l'énergie électrique véhiculée par le signal de puissance, interconnecté à l'enroulement précité.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs.

La description se réfère aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un premier mode particulier de réalisation ;

- la figure 2 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un deuxième mode particulier de réalisation ;

- la figure 3 est un organigramme du procédé de contrôle d'accès de la présente invention, dans un troisième mode particulier de réalisation ;

5 - la figure 4 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un premier mode particulier de réalisation ;

- la figure 5 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un deuxième mode particulier de réalisation ;

10 - la figure 6 représente de façon schématique le système de contrôle d'accès de la présente invention, dans un troisième mode particulier de réalisation ;

- la figure 7 reprend en partie la figure 1a de la demande de brevet français de numéro de dépôt 98 10396 ; et

15 - la figure 8 représente de façon schématique le module de transmission sans contact permettant à la clé électronique de communiquer avec la serrure électronique, dans un mode particulier de réalisation.

Dans toute la suite, on considère une clé électronique
20 utilisée pour une tentative d'accès à une serrure électronique. La clé et la serrure électroniques disposent d'une unité de calcul.

Une entité de validation extérieure est munie d'une horloge temps réel. Cette horloge temps réel délivre une valeur horaire courante VH, exprimée par exemple en jour, mois, année, heures, minutes, secondes.

On souhaite limiter l'accès de la clé à la serrure à une plage horaire donnée PH, définie comme l'intervalle de temps compris entre deux valeurs horaires VH1 et VH2 déterminées : $PH = [VH1, VH2]$, ou de manière plus large comme

une réunion de tels intervalles : PH =
[VH1, VH2] ∪ [VH3, VH4] ∪ ... ∪ [VHn-1, VHn].

Comme l'indique la figure 1, une première étape 1001 du procédé consiste à mémoriser dans la serrure électronique 5 une valeur horaire VH_s, valeur horaire courante délivrée par l'horloge temps réel de l'entité de validation précitée. Par convention, dans toute la suite, cette valeur horaire VH_s est appelée "valeur horaire de contrôle VH_s".

On considère ensuite une situation où la clé 10 électronique tente d'accéder à la serrure électronique. Cette situation peut se traduire de diverses façons, selon la forme et la nature des supports contenant la clé et la serrure. A titre d'exemple non limitatif, si la clé comporte une partie tubulaire ou en forme de languette plate, la 15 tentative d'accès se fait par introduction de la partie tubulaire dans une cavité tubulaire complémentaire de la serrure, ou dans une fente complémentaire, respectivement.

Un protocole de vérification du droit d'accès de cette clé à cette serrure est alors mis en œuvre successivement 20 dans la clé et dans la serrure.

Dans la clé, comme indiqué en 1002 sur la figure 1, on lit une plage horaire prédéterminée PH, qui a été préalablement mémorisée dans la clé électronique.

Comme indiqué en 1003, lors de la tentative d'accès, 25 on mémorise dans la clé une valeur horaire VH_c, valeur horaire courante délivrée par l'horloge temps réel de l'entité de validation précitée. Par convention, dans toute la suite, cette valeur horaire VH_c est appelée "valeur horaire d'essai VH_c".

30 Puis on transmet, en 1004, la plage de validité PH ainsi que la valeur horaire d'essai VH_c à la serrure.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 1005 et 1006, on vérifie, d'une part, la cohérence entre la valeur horaire d'essai VH_c transmise et la plage horaire prédéterminée PH , et d'autre part, la cohérence entre VH_c et la valeur horaire de contrôle VH_s mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle $[VH_1, VH_2]$, on vérifie que VH_c est postérieure à VH_1 et antérieure à VH_2 , et que VH_c est postérieure à VH_s .

Si l'une des vérifications effectuées aux étapes 1005 et 1006 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour VH_s en la remplaçant par exemple par la valeur horaire d'essai VH_c .

On décrit ci-après un autre mode de réalisation du procédé de l'invention, qui procure une sécurité accrue par rapport au mode de réalisation précédent.

On considère une ressource accédée non autonome en énergie et/ou ne disposant que d'un potentiel limité de vérification d'un droit d'accès.

Par « droit d'accès », on entend la signature électronique d'une plage de validité. Une signature électronique peut être obtenue à l'aide de mécanismes cryptographiques divers, tels que des mécanismes de chiffrement, ou d'authentification. Elle peut par exemple être obtenue à l'aide d'un algorithme de signature à clé secrète ou d'un algorithme de signature à clé publique.

Lorsqu'une « ressource accédante », ou « clé électronique », présente un droit d'accès à une « ressource accédée », ou « serrure électronique », un protocole de

vérification du droit d'accès est mis en œuvre. Dans ce mode de réalisation, ce protocole comporte, en plus de la vérification de la plage de validité, la vérification de la signature électronique de cette plage de validité.

5 Dans ce mode de réalisation, la plage de validité peut être, soit la période proprement dite pendant laquelle il est possible d'accéder à la ressource, soit la période de validité d'une clé de signature de la ressource accédante lui permettant de s'authentifier vis-à-vis de la ressource
10 accédée, soit tout autre paramètre permettant de limiter dans le temps une attaque par utilisation frauduleuse de la ressource accédante.

15 Comme l'indique la figure 2, dans ce mode de réalisation, une première étape 2001 consiste, de même qu'à l'étape 1001 dans le mode de réalisation précédent, à mémoriser dans la serrure électronique une valeur horaire de contrôle VH_s, délivrée par l'entité de validation.

20 Dans le cas où la signature électronique S utilisée est calculée à l'aide d'un algorithme à clé publique, du type RSA (Rivest Shamir Adleman) par exemple, on mémorise dans la serrure électronique la clé publique K_p de vérification de la signature. Cette clé publique de vérification K_p devra être stockée de façon qu'elle ne puisse pas être modifiée par une entité non autorisée. La
25 clé K_p sera le cas échéant stockée dans une mémoire physiquement protégée.

30 La signature électronique S peut également être calculée à l'aide d'un algorithme à clé secrète, du type DES (Data Encryption Standard) par exemple. Dans ce cas, contrairement au cas précédent, la clé de vérification qui est mémorisée dans la serrure à l'étape 2001 est secrète. De ce fait, elle devra être stockée dans une mémoire

physiquement protégée, de sorte qu'elle ne puisse être ni lue, ni modifiée par une entité non autorisée.

On considère ensuite une situation où la clé électronique tente d'accéder à la serrure électronique. De 5 même que dans le mode de réalisation précédent, un protocole de vérification du droit d'accès de cette clé à cette serrure est mis en œuvre successivement dans la clé et dans la serrure.

Dans la clé, comme indiqué en 2002 sur la figure 2, on 10 lit ou on établit une signature électronique $S(PH)$ de la plage horaire prédéterminée PH . Cette étape a lieu, soit en plus, soit en lieu et place de l'étape 1002 de lecture de la plage horaire PH du mode de réalisation précédent.

Cette signature électronique $S(PH)$ peut avoir été 15 calculée au préalable, par exemple par une entité extérieure de calcul de signatures, indépendante de la clé.

Dans ce cas, lors d'une étape de chargement, par exemple au moyen d'une borne de validation, l'entité de validation précitée transfère et mémorise la signature $S(PH)$ 20 dans la clé avant que cette clé soit mise en service.

En variante, la clé peut établir elle-même la signature, si on a mémorisé dans la clé électronique la clé privée nécessaire à cette opération, ainsi que l'algorithme 25 cryptographique de signature, et si cette clé dispose des ressources calculatoires nécessaires.

Comme indiqué en 2003, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire d'essai VH_c délivrée par l'entité de validation.

Puis on transmet, en 2004, la signature électronique 30 $S(PH)$ de la plage de validité ainsi que la valeur horaire d'essai VH_c à la serrure. Si, à l'étape 2002, on a lu la plage horaire PH en plus de la signature $S(PH)$, on transmet

également cette plage horaire PH à la serrure à l'étape 2004.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

- 5 En 2005, on vérifie la signature transmise. Si l'algorithme de calcul de signatures est un algorithme à clé publique, l'étape 2005 consiste, pour la serrure électronique, à appliquer la clé publique K_p , préalablement mémorisée dans la serrure, à l'algorithme de vérification.
- 10 La vérification positive de la signature permet d'assurer l'authenticité de la plage de validité [VH₁, VH₂], ladite plage étant obtenue, soit par rétablissement du message au cours de l'étape de vérification de signature, soit par simple lecture si elle a été transmise en clair avec la
- 15 signature.

En 2006 et 2007, on vérifie, d'une part, la cohérence entre la valeur horaire d'essai VH_c transmise et la plage horaire prédéterminée PH, et d'autre part, la cohérence entre VH_c et la valeur horaire de contrôle VH_s mémorisée dans la serrure.

Par exemple, dans le cas d'une plage horaire réduite à un intervalle [VH₁, VH₂], on vérifie que VH_c est postérieure à VH₁ et antérieure à VH₂, et que VH_c est postérieure à VH_s.

Si l'une des vérifications effectuées aux étapes 2005, 2006 et 2007 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour VH_s en la remplaçant par exemple par la valeur horaire d'essai VH_c.

30 On décrit ci-dessous à l'aide de la figure 3 un troisième mode de réalisation du procédé de l'invention, qui

est susceptible de procurer une sécurité accrue par rapport aux modes de réalisation précédents.

Les étapes 3001 et 3002 illustrées sur la figure 3 sont respectivement identiques aux étapes 2001 et 2002 du mode de réalisation précédent et ne seront pas décrites à nouveau.

Comme indiqué en 3003 sur la figure 3, lors de la tentative d'accès, on mémorise dans la clé la valeur horaire d'essai VH_c délivrée par l'entité de validation. De plus, on calcule et on mémorise dans la clé une signature électronique $S(VH_c)$ de la valeur horaire d'essai VH_c reçue en provenance de l'entité de validation.

En variante, cette signature électronique $S(VH_c)$ peut être calculée par une unité de calcul de signatures indépendante de la clé, par exemple contenue dans l'entité de validation.

Dans ce cas, lors de la délivrance de la valeur horaire d'essai VH_c , l'entité de validation transfère et mémorise également la signature $S(VH_c)$ dans la clé.

En variante, la clé peut établir elle-même la signature de la valeur d'essai VH_c , si on a mémorisé dans la clé électronique la clé privée nécessaire à cette opération, ainsi que l'algorithme cryptographique de signature, et si cette clé dispose des ressources calculatoires nécessaires.

Puis on transmet à la serrure, en 3004, les signatures électroniques $S(PH)$ de la plage de validité PH et $S(VH_c)$ de la valeur horaire d'essai VH_c , ainsi que la valeur horaire d'essai VH_c . Si, à l'étape 3002, on a lu la plage horaire PH en plus de la signature $S(PH)$, on transmet également cette plage horaire PH à la serrure à l'étape 3004.

Les étapes suivantes de vérification ont alors lieu dans la serrure.

En 3005, on vérifie les signatures $S(PH)$ et $S(VH_c)$ transmises, par exemple au moyen d'un même algorithme de vérification. Si l'algorithme de calcul de signatures est un algorithme à clé publique, l'étape 3005 consiste, pour la 5 serrure électronique, à appliquer la clé publique K_p , préalablement mémorisée dans la serrure, à l'algorithme de vérification.

La vérification positive de la signature $S(PH)$ permet d'assurer l'authenticité de la plage de validité $[VH_1, VH_2]$, 10 cette plage étant obtenue, soit par rétablissement du message au cours de l'étape de vérification de signature, soit par simple lecture si elle a été transmise en clair avec la signature.

La vérification positive de la signature $S(VH_c)$ permet 15 d'assurer l'authenticité de la valeur horaire d'essai VH_c .

Les étapes suivantes 3006 et 3007 sont respectivement identiques aux étapes 2006 et 2007 du mode de réalisation précédent et ne seront pas décrites à nouveau.

Si l'une des vérifications effectuées aux étapes 3005, 20 3006 et 3007 donne lieu à une réponse négative, on interdit l'accès de cette clé à cette serrure.

Si l'ensemble de ces vérifications a été satisfait, on autorise l'accès, et on met à jour VH_s en la remplaçant par exemple par la valeur horaire d'essai VH_c , de même que dans 25 les modes de réalisation précédents.

Un mode particulier de réalisation du système de contrôle d'accès conforme à la présente invention va maintenant être décrit à l'aide de la figure 4.

Le système comprend une clé électronique 1 et une 30 serrure électronique 2.

La clé électronique 1 comprend une mémoire 13, dans laquelle sont mémorisées la plage de validité PH et une

valeur horaire d'essai VH_c , telle que celle délivrée par l'entité de validation extérieure (non représentée sur la figure 4) dans le cadre du procédé de contrôle d'accès décrit ci-dessus.

5 La mémoire 13 est reliée à un module 14 de communication de la clé avec la serrure. Le module 14 permet à la clé, lors de chaque tentative d'accès, de transmettre à un module 21 de communication compris dans la serrure 2 la plage horaire PH ainsi que la valeur horaire d'essai VH_c
10 délivrée par l'entité de validation, les valeurs PH et VH_c étant mémorisées dans la mémoire 13.

Le module 21 de communication de la serrure avec la clé est relié à une mémoire 22 accessible en lecture et en écriture, dans laquelle est mémorisée une valeur horaire de
15 contrôle VH_s , telle que celle délivrée par l'entité de validation extérieure dans le cadre du procédé de contrôle d'accès décrit ci-dessus.

La valeur horaire de contrôle VH_s est remise à jour, par exemple à l'aide de la valeur horaire d'essai VH_c
20 transmise par la clé 1, à chaque tentative d'accès réussie.

La mémoire 22 est par exemple une mémoire reprogrammable électriquement du type EPROM ou EEPROM.

La clé électronique 1 peut, à titre d'exemple non limitatif, être réalisée sous une forme analogue à celle
25 d'un ensemble décrit en relation avec la figure 1a de la demande de brevet français de numéro de dépôt 98 10396, reprise sur la figure 7 de la présente demande. Le contenu de la demande n° 98 10396 précitée est incorporé par référence dans la présente description.

30 Comme le montre la figure 7 de la présente demande, la clé électronique 1 comporte un module d'émission - réception l_2 de signaux de contrôle d'accès de clé. Ce module l_2 peut

comprendre, de manière avantageuse, un module d'émission des signaux de contrôle d'accès de clé et un module de réception des signaux de contrôle d'accès de serrure. Par convention, les signaux de contrôle d'accès de clé désignent les signaux de contrôle d'accès émis par la clé vers la serrure et les signaux de contrôle d'accès de serrure désignent les signaux de contrôle d'accès émis par la serrure vers la clé.

La clé électronique 1 comporte en outre, comme indiqué plus haut, une unité de calcul, dite unité logique de calcul de clé l_1 . L'unité logique de calcul de clé l_1 permet de contrôler l'ensemble des opérations de fonctionnement de la clé électronique 1.

La serrure électronique 2 comporte également, comme indiqué plus haut, une unité de calcul, dite unité logique de calcul de serrure 2_1 , et un module d'émission - réception 2_2 de signaux de contrôle d'accès de serrure.

De façon classique, l'unité logique de calcul de serrure 2_1 permet également de contrôler l'ensemble des opérations de fonctionnement de la serrure électronique 2.

Ainsi, sous le contrôle respectif des unités logiques de calcul de clé et de serrure l_1 et 2_1 , les modules d'émission - réception des signaux de contrôle d'accès de clé et de serrure l_2 et 2_2 permettent la mise en œuvre d'un protocole de contrôle d'accès entre la clé électronique 1 et la serrure électronique 2.

L'ensemble représenté sur la figure 7 de la présente demande comporte en outre, au niveau de la clé électronique 1, un module l_3 générateur d'un signal de puissance.

Le module de puissance l_3 peut être alimenté par une source d'énergie électrique extérieure (non représentée). En variante, mais non nécessairement, le module de puissance l_3 peut être alimenté par un module optionnel d'alimentation en

énergie 11, représenté sur les figures 4, 5 et 6 de la présente demande, à titre d'exemple nullement limitatif.

Le module de puissance 1₃ peut être piloté par l'unité logique de calcul de clé 1₁.

5 Ainsi, l'ensemble des modules fonctionnels d'émission - réception 1₂ de signaux de contrôle d'accès de clé et générateur de puissance 1₃ est connecté par une liaison à l'unité logique de calcul de clé 1₁ et piloté par cette dernière.

10 En outre, comme le montre la figure 7, la clé électronique 1 comprend un premier circuit de transfert dit circuit de transfert de clé 1₄, permettant notamment le transfert des signaux de contrôle d'accès de clé et de serrure ainsi que du signal de puissance engendré par le 15 module de puissance 1₃. Plus précisément, le circuit de transfert de clé 1₄ est relié, d'une part, au module de puissance 1₃ et d'autre part, au module d'émission - réception de signaux de contrôle d'accès de clé 1₂.

20 Comme le montre la figure 7, la serrure électronique 2 comporte un second circuit de transfert, dit circuit de transfert de serrure 2₄, permettant notamment le transfert des signaux de contrôle d'accès de clé et de serrure et du signal de puissance mentionné précédemment.

25 De plus, la serrure électronique 2 comprend également un module 2₅ permettant d'assurer le stockage et donc la récupération de l'énergie électrique véhiculée par le signal de puissance.

30 Comme le montre de façon non limitative la figure 7, la serrure 2 peut être en outre munie d'un module 2₃ de récupération d'un signal d'horloge.

Les modules fonctionnels constitutifs de la serrure électronique 2, c'est-à-dire, dans le mode particulier de

réalisation de la figure 7, le module d'émission - réception des signaux de contrôle d'accès de serrure 2₂, le module de stockage de l'énergie électrique 2₅ et, le cas échéant, le module de récupération d'horloge 2₃, sont connectés par 5 l'intermédiaire d'une liaison à l'unité logique de calcul de serrure 2₁.

Le circuit de transfert de serrure 2₄ est relié, d'une part, au module d'émission - réception 2₂ des signaux de contrôle d'accès de serrure et d'autre part, au module 2₅ de 10 stockage de l'énergie électrique ainsi que, le cas échéant, au module 2₃ de récupération d'horloge.

D'une manière avantageuse non limitative, comme le montre la figure 7, le circuit de transfert 1₄ de la clé et le circuit de transfert 2₄ de la serrure peuvent être 15 constitués par l'enroulement primaire et l'enroulement secondaire d'un transformateur. Dans de telles conditions, les enroulements primaire, noté L₁, et secondaire, noté L₂, sont couplés du point de vue électromagnétique lors de la mise en présence de la clé électronique et de la serrure 20 électronique, cette mise en présence étant effectuée pour réaliser une tentative d'accès.

Comme le montre la figure 4, la serrure 2 comprend en outre un module 25 de comparaison, qui reçoit la valeur horaire d'essai VH_c transmise par la clé 1, et la compare à 25 la plage horaire prédefinie PH = [VH₁, VH₂] et à la valeur horaire de contrôle VH_s mémorisée dans la mémoire 22. Le module 25 de comparaison teste si VH_c > VH₁ et VH_c < VH₂, et si VH_c > VH_s.

Dans un mode particulier de réalisation, comme indiqué 30 plus haut, la clé 1 peut comprendre en outre un module 11 d'alimentation en énergie pour fournir à la serrure 2 l'énergie nécessaire aux opérations de vérification

effectuées par le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour de la valeur horaire de contrôle VH_s mémorisée dans la mémoire 22 en cas de tentative d'accès réussie.

5 En variante, la clé 1 ne comprend aucun module d'alimentation en énergie et l'énergie nécessaire aux opérations de vérification et de remise à jour est fournie par une source d'énergie électrique extérieure.

On décrit ci-après, à l'aide de la figure 5, un autre 10 mode de réalisation du système de contrôle d'accès de l'invention, comprenant une clé électronique 41 et une serrure électronique 42, qui procure une sécurité accrue par rapport au mode de réalisation de la figure 4.

Les éléments de ce système qui sont analogues à ceux 15 du mode de réalisation de la figure 4 portent les mêmes chiffres de référence, et ne seront pas décrits une nouvelle fois.

Dans ce mode de réalisation, la mémoire 13 de la clé 41 contient non seulement la plage de validité PH, mais 20 aussi la signature électronique S(PH) de cette plage de validité.

La module 14 de communication de la clé avec la serrure permet à la clé 41, lors de chaque tentative 25 d'accès, de transmettre au module 21 de communication compris dans la serrure 42, non seulement la valeur horaire d'essai VH_c et la plage horaire PH, mémorisées dans la mémoire 13, mais aussi la signature électronique S(PH) mémorisée dans la mémoire 13.

La serrure 42 comprend, en plus du module 21 de 30 communication avec la clé, de la mémoire 22 et du module 25 de comparaison, décrits précédemment, un module 24 de vérification de signature.

Le module 24 est relié au module 21 de communication de la serrure avec la clé et au module 25 de comparaison. Le module 24 reçoit la signature S(PH) de la plage de validité et, dans le cas où l'algorithme de calcul de signatures utilisé est un algorithme à clé publique, vérifie la signature S(PH) reçue au moyen de la clé publique K_p.

De même que précédemment, dans un mode particulier de réalisation, la clé 41 peut comprendre en outre un module 11 d'alimentation en énergie, pour fournir à la serrure 42 l'énergie nécessaire aux opérations de vérification effectuées par le module 24 de vérification de signature et le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour de la valeur horaire de contrôle VH_s mémorisée dans la mémoire 22 en cas de tentative d'accès réussie.

En variante, la clé 41 ne comprend aucun module d'alimentation en énergie et l'énergie nécessaire aux opérations de vérification et de remise à jour est fournie par une source d'énergie électrique extérieure.

On décrit ci-après, à l'aide de la figure 6, un troisième mode de réalisation du système de contrôle d'accès de l'invention, comprenant également une clé électronique 41 et une serrure électronique 42, qui est susceptible de procurer une sécurité accrue par rapport aux modes de réalisation précédents.

Les éléments de ce système qui sont analogues à ceux du mode de réalisation de la figure 5 portent les mêmes chiffres de référence, et ne seront pas décrits une nouvelle fois.

Dans ce mode de réalisation, la mémoire 13 de la clé 41 contient non seulement la plage de validité PH et la signature électronique S(PH) de cette plage de validité,

mais aussi la signature électronique $S(VH_c)$ de la valeur horaire d'essai.

La module 14 de communication de la clé avec la serrure permet à la clé 41, lors de chaque tentative 5 d'accès, de transmettre au module 21 de communication compris dans la serrure 42, non seulement la valeur horaire d'essai VH_c , la plage horaire PH et la signature électronique $S(PH)$, mémorisées dans la mémoire 13, mais aussi la signature électronique $S(VH_c)$ mémorisée dans la 10 mémoire 13.

Le module 24 de vérification de signature reçoit les signatures $S(PH)$ de la plage de validité et $S(VH_c)$ de la valeur d'essai, dans le cas où l'algorithme de calcul de signatures utilisé est un algorithme à clé publique, vérifie 15 ces signatures au moyen de la clé publique K_p .

De même que précédemment, dans un mode particulier de réalisation, la clé 41 peut comprendre en outre un module 11 d'alimentation en énergie, pour fournir à la serrure 42 l'énergie nécessaire aux opérations de vérification 20 effectuées par le module 24 de vérification de signature et le module 25 de comparaison, ainsi que l'énergie nécessaire à l'opération de remise à jour de la valeur horaire de contrôle VH_s mémorisée dans la mémoire 22 en cas de tentative d'accès réussie.

25 En variante, la clé 41 ne comprend aucun module d'alimentation en énergie et l'énergie nécessaire aux opérations de vérification et de remise à jour est fournie par une source d'énergie électrique extérieure.

La figure 8 illustre une réalisation matérielle 30 particulière des modules 14 et 21 de communication entre la clé et la serrure, applicable aussi bien au mode de

réalisation de la figure 4 qu'aux modes de réalisation des figures 5 et 6.

La clé 1 (ou 41 dans le cas des modes de réalisation des figures 5 et 6) comprend une tige 30 en matière ferromagnétique, garnie d'enroulements en cuivre 31 formant un premier bobinage. Ce premier bobinage est relié au module 14 de communication de la clé avec la serrure.

A chaque tentative d'accès, la clé 1 ou 41 vient se loger dans une cavité tubulaire 32 de diamètre légèrement supérieur au diamètre de la tige 30. La cavité 32 est également garnie d'enroulements en cuivre 33 formant un second bobinage, relié au module 21 de communication de la serrure avec la clé. Les deux bobinages 31, 33 sont alors concentriques, et l'information est transmise sous forme codée binaire entre la clé et la serrure 2 (ou 42 dans le cas du mode de réalisation de la figure 5) par induction électromagnétique.

La présente invention trouve une application particulièrement adaptée à l'accès, par des utilisateurs successifs, à des ressources qui ne sont rendues accessibles à un utilisateur donné qu'après avoir été libérées par un utilisateur précédent, et qui, après l'accès réalisé de cet utilisateur donné, ne permet plus l'accès à l'utilisateur précédent. On peut ainsi appliquer l'invention à des ressources telles que des chambres d'hôtel ou des casiers de consigne automatique.

On peut renforcer encore davantage la sécurité du contrôle d'accès, en ajoutant d'autres données aux informations de signature et de plage horaire transmises par la clé à la serrure. Par exemple, on peut ajouter un numéro de série identifiant la clé électronique. Dans ce cas, on peut munir la serrure d'un module de comptage, associé à ce

numéro de série. On mémorise dans ce module de comptage le début de la prochaine plage horaire au cours de laquelle une clé portant ce numéro de série pourra accéder à la serrure.

REVENDICATIONS

1. Procédé de contrôle d'accès d'au moins une clé électronique à au moins une serrure électronique, à l'intérieur d'une plage horaire prédéterminée, suivant lequel :

(a) préalablement à toute tentative d'accès de la clé électronique à une serrure électronique, on mémorise dans la serrure une valeur horaire de contrôle (VH_s), délivrée par une horloge temps réel d'une entité de validation extérieure ;

puis, lors de chaque tentative d'accès de la clé électronique à une serrure électronique :

dans la clé électronique :

(b) on lit une plage horaire (PH) prédéterminée, préalablement mémorisée dans la clé électronique ;

(c) on mémorise dans la clé une valeur horaire d'essai (VH_c), délivrée par l'horloge temps réel de ladite entité de validation extérieure ;

(d) on transmet de la clé électronique à la serrure électronique la plage horaire (PH) et la valeur horaire d'essai (VH_c), et

dans la serrure électronique :

(e) on vérifie que la valeur horaire d'essai (VH_c) transmise est à l'intérieur de la plage horaire (PH) prédéterminée, et qu'elle est postérieure à la valeur horaire de contrôle (VH_s) mémorisée dans la serrure ;

(f) si les vérifications effectuées à l'étape (e) sont satisfaites, on autorise l'accès, et on met à jour la valeur horaire de contrôle (VH_s), à partir de la valeur horaire d'essai (VH_c) transmise ;

(g) si la valeur horaire d'essai (VH_c) transmise est à l'extérieur de la plage horaire (PH) prédéterminée, ou si elle est antérieure à la valeur horaire de contrôle (VH_s) mémorisée dans la serrure, on interdit l'accès de cette clé 5 à cette serrure.

2. Procédé selon la revendication 1, caractérisé en ce que :

dans la clé électronique :

(b1) à l'étape (b), on lit, en plus de la plage 10 horaire (PH), ou en lieu et place de la plage horaire (PH), une signature électronique ($S(PH)$) de ladite plage horaire (PH), préalablement calculée et mémorisée dans la clé électronique ;

(d1) à l'étape (d), on transmet de la clé 15 électronique à la serrure électronique, d'une part, ladite signature électronique ($S(PH)$) en plus ou en lieu et place de la plage horaire (PH), et, d'autre part, de ladite valeur horaire d'essai (VH_c), et

dans la serrure électronique :

(e1) avant l'étape (e), on vérifie la signature 20 transmise ($S(PH)$), à partir d'une clé de vérification spécifique ;

(f1) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur horaire de contrôle (VH_s), à partir 25 de la valeur horaire d'essai (VH_c) transmise, que si les vérifications effectuées aux étapes (e1) et (e) sont satisfaites ;

(g1) à l'étape (g), on interdit l'accès de ladite clé à ladite serrure si la valeur horaire d'essai (VH_c) 30 transmise est à l'extérieur de ladite plage horaire (PH), ou si elle est antérieure à la valeur horaire de contrôle (VH_s)

mémorisée dans la serrure, ou si la vérification effectuée à l'étape (e1) n'est pas satisfaite.

3. Procédé selon la revendication 2, caractérisé en ce que l'ordre d'exécution des étapes (e1) et (e) est 5 interverti.

4. Procédé selon la revendication 2 ou 3, caractérisé en ce que ladite clé de vérification spécifique est une clé publique ou secrète.

5. Procédé selon l'une quelconque des revendications 10 précédentes, caractérisé en ce que :

dans la clé électronique :

(c2) à l'étape (c), on calcule et on mémorise, en plus de la valeur horaire d'essai (VH_c), une signature électronique ($S(VH_c)$) de cette valeur horaire d'essai ;

15 (d2) à l'étape (d1), on transmet en outre, de la clé électronique à la serrure électronique, ladite signature électronique ($S(VH_c)$) de la valeur horaire d'essai (VH_c), et

dans la serrure électronique :

20 (e2) avant ou après l'étape (e), on vérifie la signature ($S(VH_c)$) de la valeur d'essai, à partir d'une seconde clé de vérification spécifique publique ou secrète ;

(f2) à l'étape (f), on n'autorise l'accès, et on ne met à jour la valeur horaire de contrôle (VH_s), que si les vérifications effectuées aux étapes (e), (e1) et (e2) 25 sont satisfaites ;

(g2) à l'étape (g), on interdit l'accès de ladite clé à ladite serrure si l'une des vérifications effectuées aux étapes (e), (e1) ou (e2) n'est pas satisfaite.

6. Procédé selon l'une quelconque des revendications 30 précédentes, caractérisé en ce que ladite plage horaire prédéterminée comprend plusieurs plages horaires disjointes.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce chaque plage horaire est un intervalle comportant deux bornes exprimées chacune comme une date en jour, mois, année et un horaire en heures, 5 minutes, secondes.

8. Système de contrôle d'accès électronique, à l'intérieur d'une plage horaire prédéterminée, comportant au moins une serrure électronique (2;42) et au moins une clé électronique (1;41), caractérisé en ce que

10 la clé (1;41) comprend :

- des moyens (13) de mémorisation d'une valeur horaire d'essai (VH_c), accessibles en lecture et en écriture, et

15 - des moyens (14) de communication pour transmettre à la serrure (2;42) une plage horaire (PH) prédéterminée et ladite valeur horaire d'essai (VH_c), et en ce que

la serrure (2;42) comprend :

- des moyens (22) de mémorisation d'une valeur horaire de contrôle (VH_s), accessibles en lecture et en écriture, et

- des moyens (25) de comparaison de la valeur horaire d'essai (VH_c) à la plage horaire (PH) prédéterminée et à la valeur horaire de contrôle (VH_s) mémorisée dans lesdits moyens (22) de mémorisation de la serrure.

25 9. Système selon la revendication 8, caractérisé en ce que

- lesdits moyens (14) de communication de la clé électronique (1;41) comprennent en outre des moyens pour transmettre à la serrure (2;42) une signature électronique (S(PH)) de ladite plage horaire (PH) et une signature électronique (S(VH_c)) de ladite valeur horaire d'essai (VH_c), et en ce que

- la serrure (2;42) comprend en outre des moyens (24) pour vérifier les signatures électroniques ($S(PH)$, $S(VH_c)$) transmises par la clé (1;41).

10. Système selon la revendication 8 ou 9, caractérisé 5 en ce que lesdits moyens (22) de mémorisation comprennent une mémoire non volatile reprogrammable électriquement.

11. Système selon la revendication 8, 9 ou 10, caractérisé en ce que la clé électronique (1;41) communique avec la serrure électronique (2;42) à l'aide de moyens de 10 transmission sans contact, par induction électromagnétique.

12. Système selon la revendication 11, caractérisé en ce que lesdits moyens de transmission sans contact comprennent un premier bobinage électromagnétique (31) prévu dans la clé (1;41) et un second bobinage électromagnétique 15 (33) prévu dans la serrure (2;42).

13. Système selon la revendication 12, caractérisé en ce que les bobinages (31,33) prévus dans la clé (1;41) et dans la serrure (2;42) sont concentriques.

14. Dans un système de contrôle d'accès électronique à 20 l'intérieur d'une plage horaire prédéterminée comportant au moins une clé électronique et une serrure électronique selon l'une des revendications 8 à 13, une clé électronique (1;41) comportant au moins une unité logique de calcul de clé (l_1), un module (l_2) d'émission - réception de signaux de contrôle 25 d'accès de clé pour la mise en œuvre d'un procédé de contrôle d'accès entre cette clé électronique (1;41) et une serrure électronique (2;42) à partir de signaux de contrôle d'accès de serrure engendrés par cette serrure électronique (2;42), caractérisée en ce que cette clé électronique 30 comporte en outre :

- des moyens (1₃) générateurs d'un signal de puissance, pilotés par ladite unité de calcul de clé (1₁) ; et

5 - des moyens de transfert de clé desdits signaux de contrôle d'accès de clé et de serrure et dudit signal de puissance, lesdits moyens de transfert de clé comportant au moins un enroulement (L₁) interconnecté auxdits moyens (1₃) générateurs d'un signal de puissance et audit module (1₂) d'émission - réception.

10 15. Dans un système de contrôle d'accès électronique à l'intérieur d'une plage horaire prédéterminée comportant au moins une clé électronique et une serrure électronique selon l'une des revendications 8 à 13, une serrure électronique (2;42) comportant au moins une unité logique de calcul de 15 serrure (2₁) et un module (2₂) d'émission - réception de signaux de contrôle d'accès de serrure pour la mise en œuvre d'un procédé de contrôle d'accès entre cette serrure électronique (2;42) et une clé électronique (1;41) à partir de 20 signaux de contrôle d'accès de clé et d'un signal de puissance engendrés par cette clé électronique, caractérisée en ce que cette serrure électronique comporte en outre :

- des moyens de transfert de serrure desdits signaux de contrôle d'accès de clé et de serrure et dudit signal de puissance, lesdits moyens de transfert de serrure comportant 25 au moins un enroulement (L₂) interconnecté audit module (2₂) d'émission - réception de signaux de contrôle d'accès de serrure ; et

- des moyens (2₅) de stockage de l'énergie électrique véhiculée par ledit signal de puissance, 30 interconnectés audit enroulement (L₂).

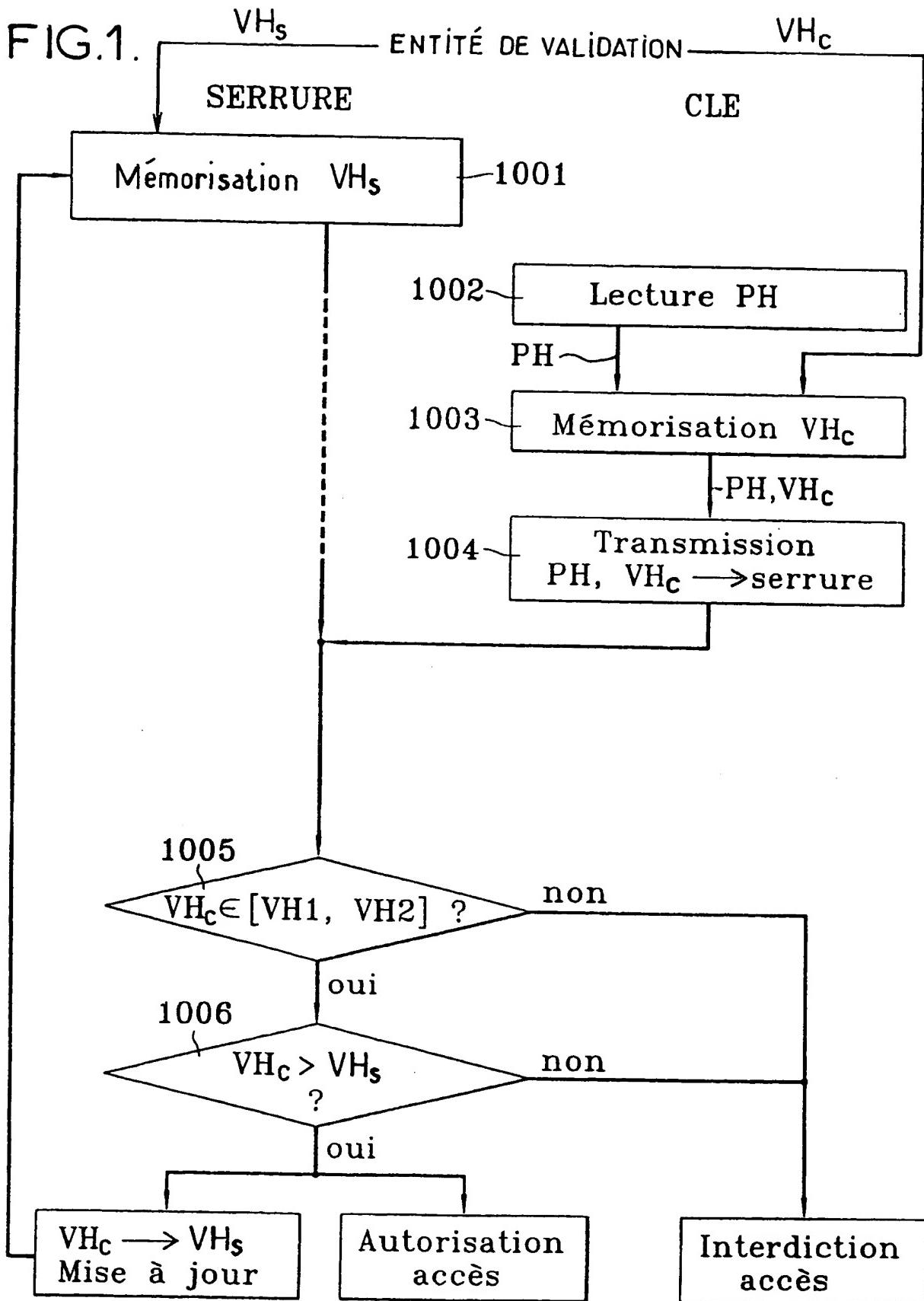


FIG.2.

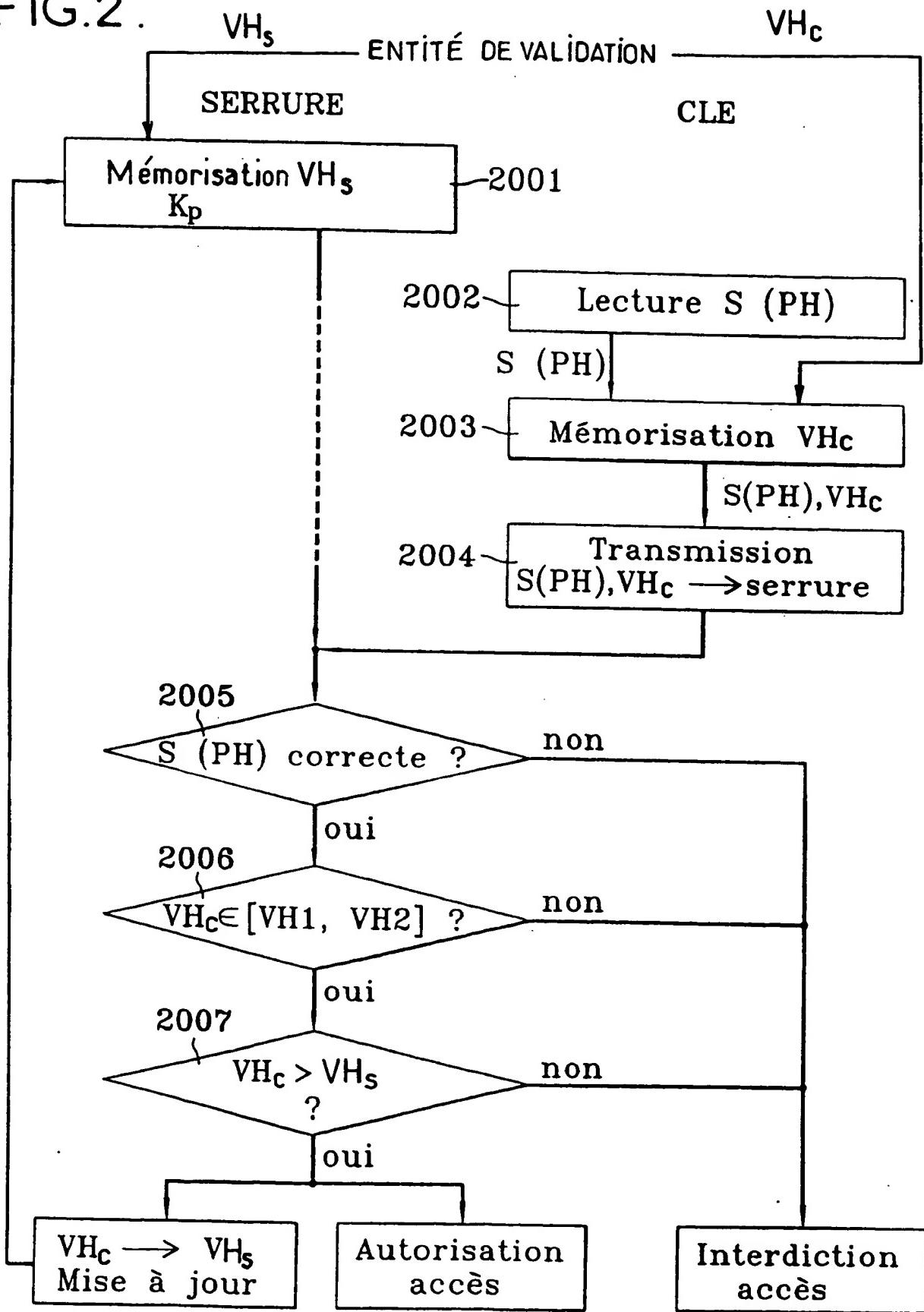
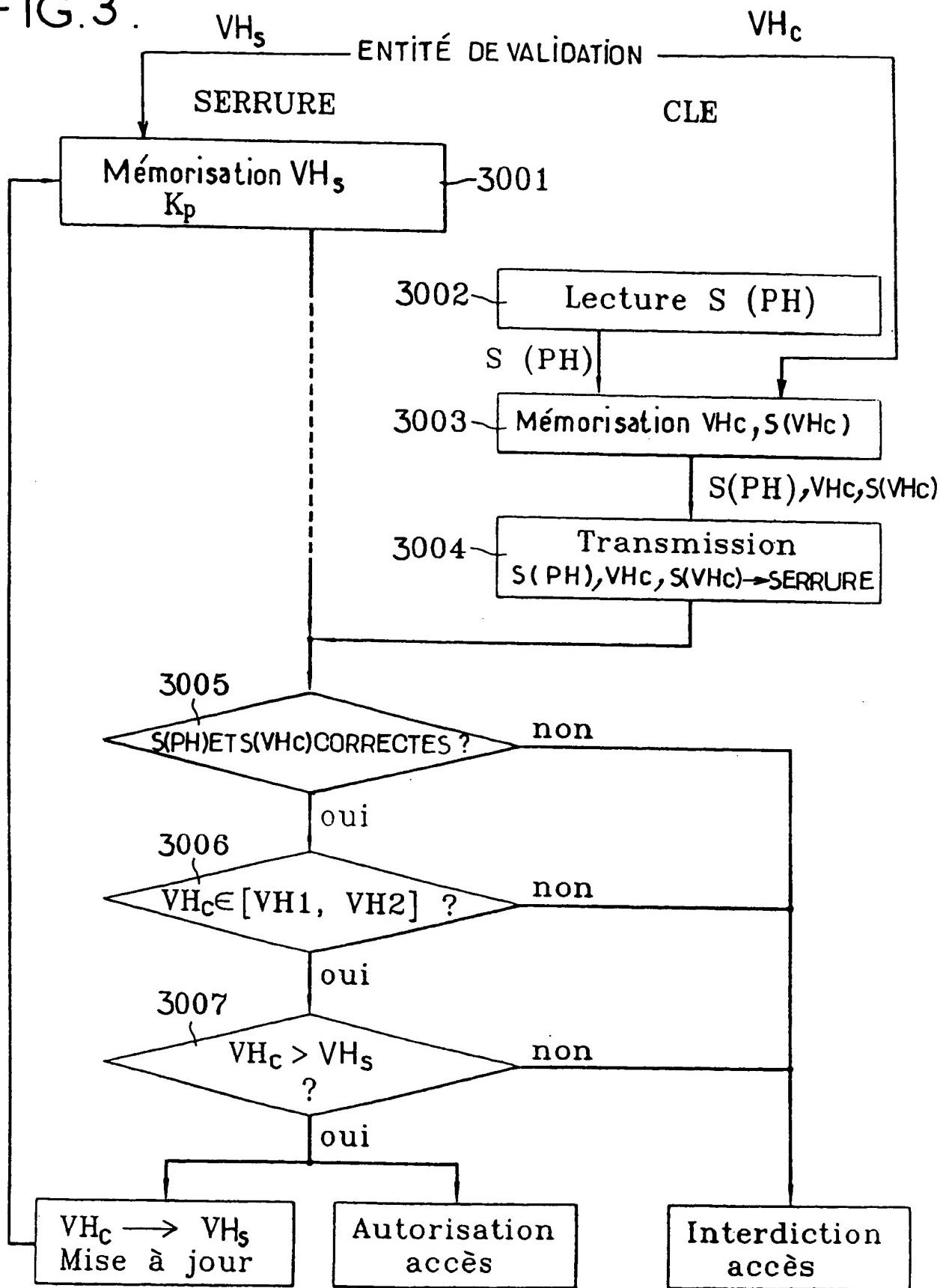
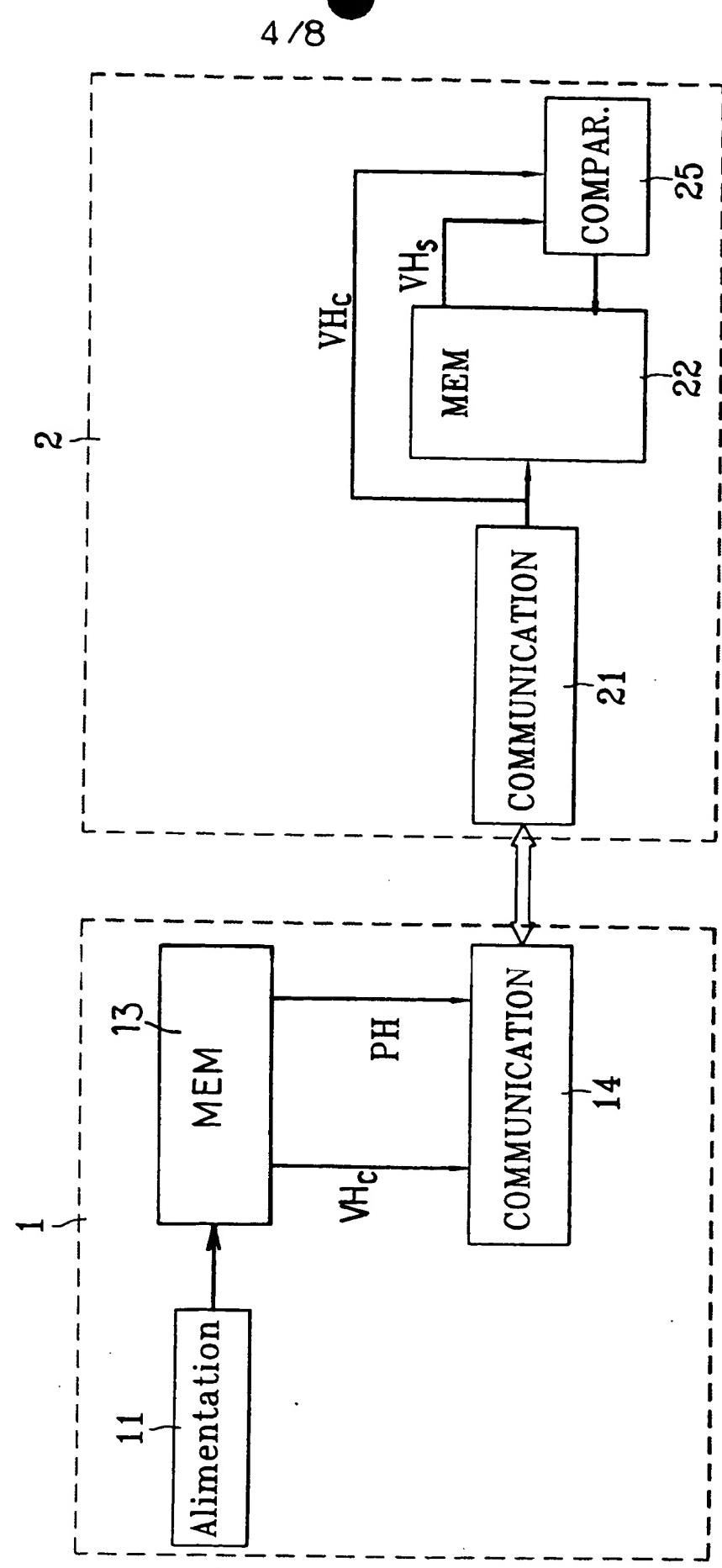


FIG.3.



CLE

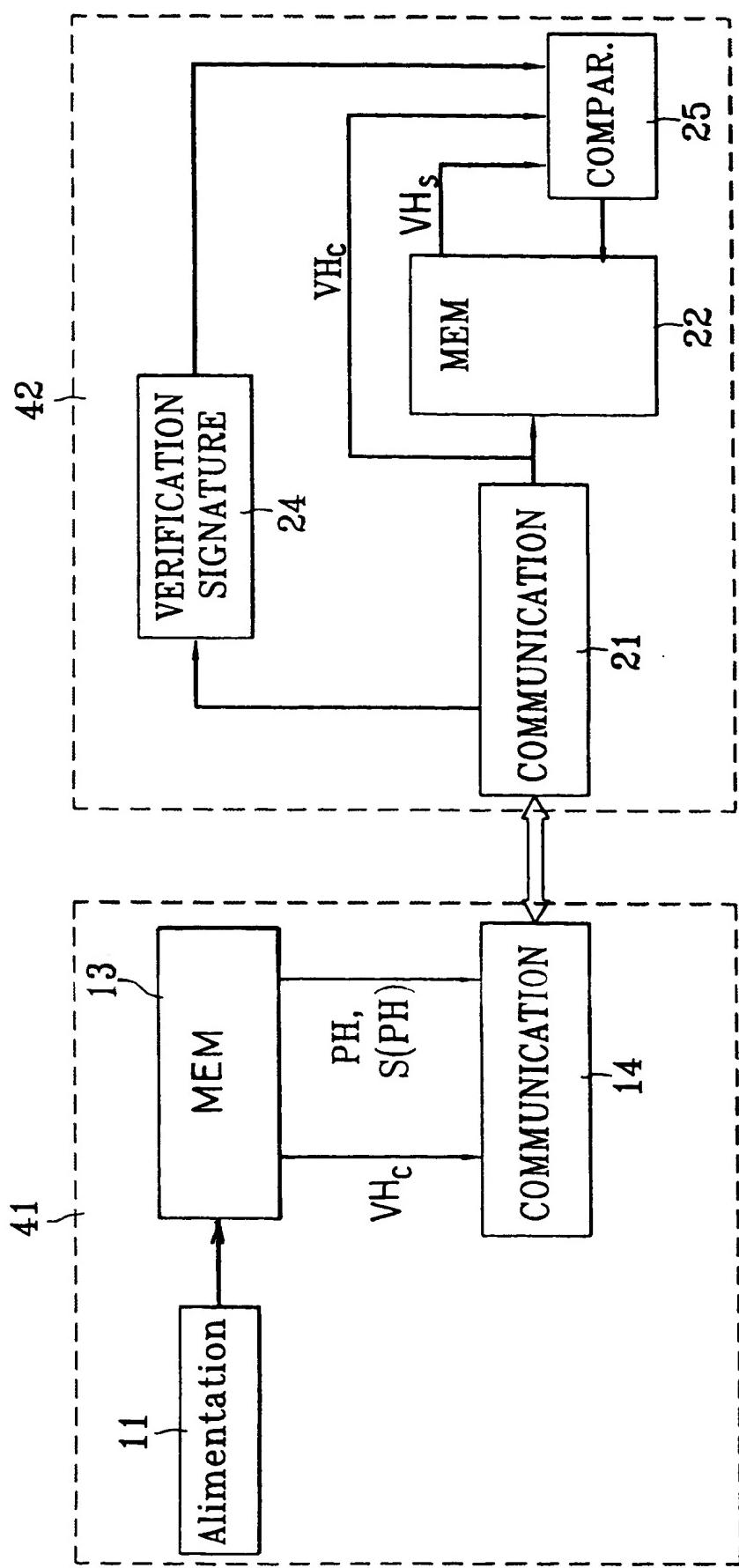
FIG.4 .
SERRURE



CLE

FIG. 5.

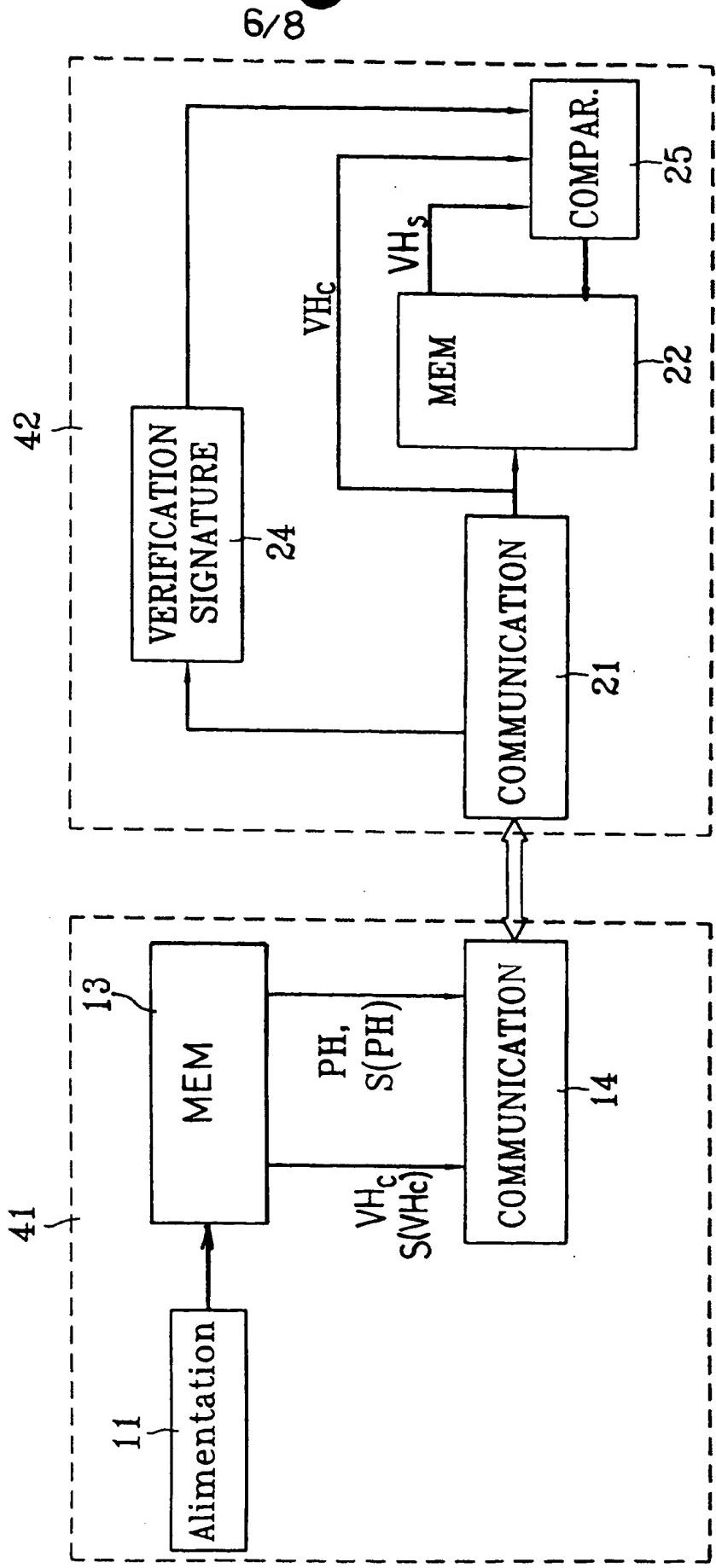
5/8



CLE

FIG.6.

SERRURE



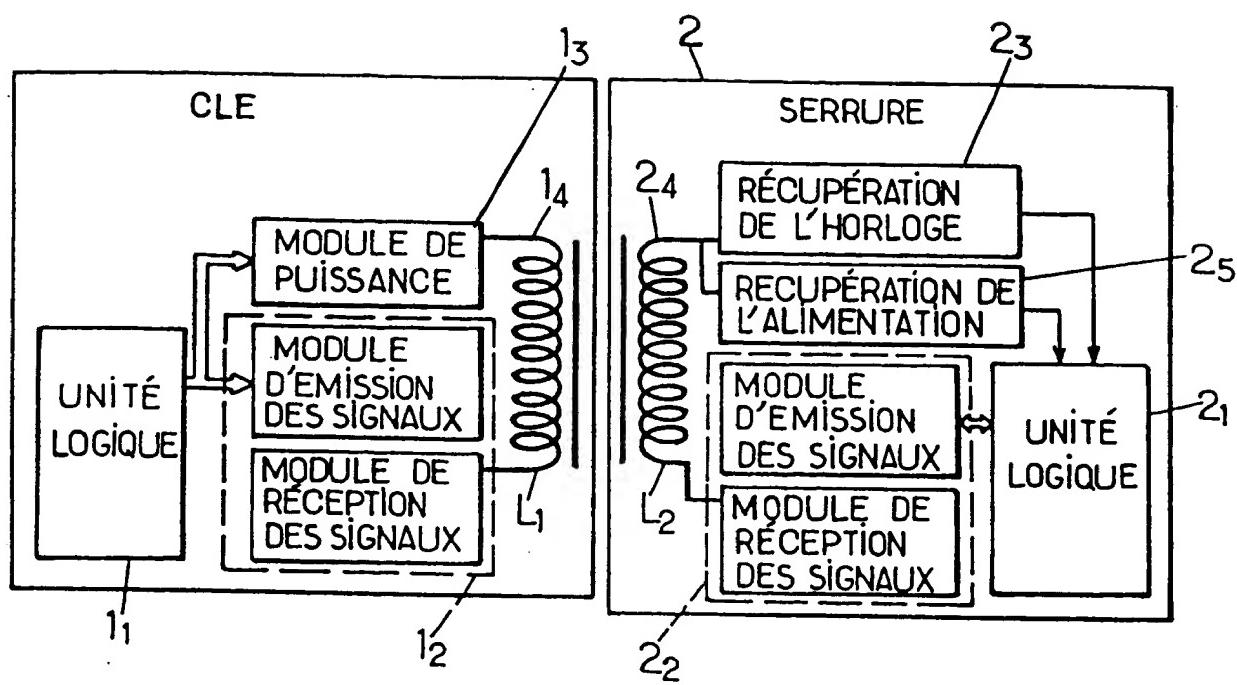
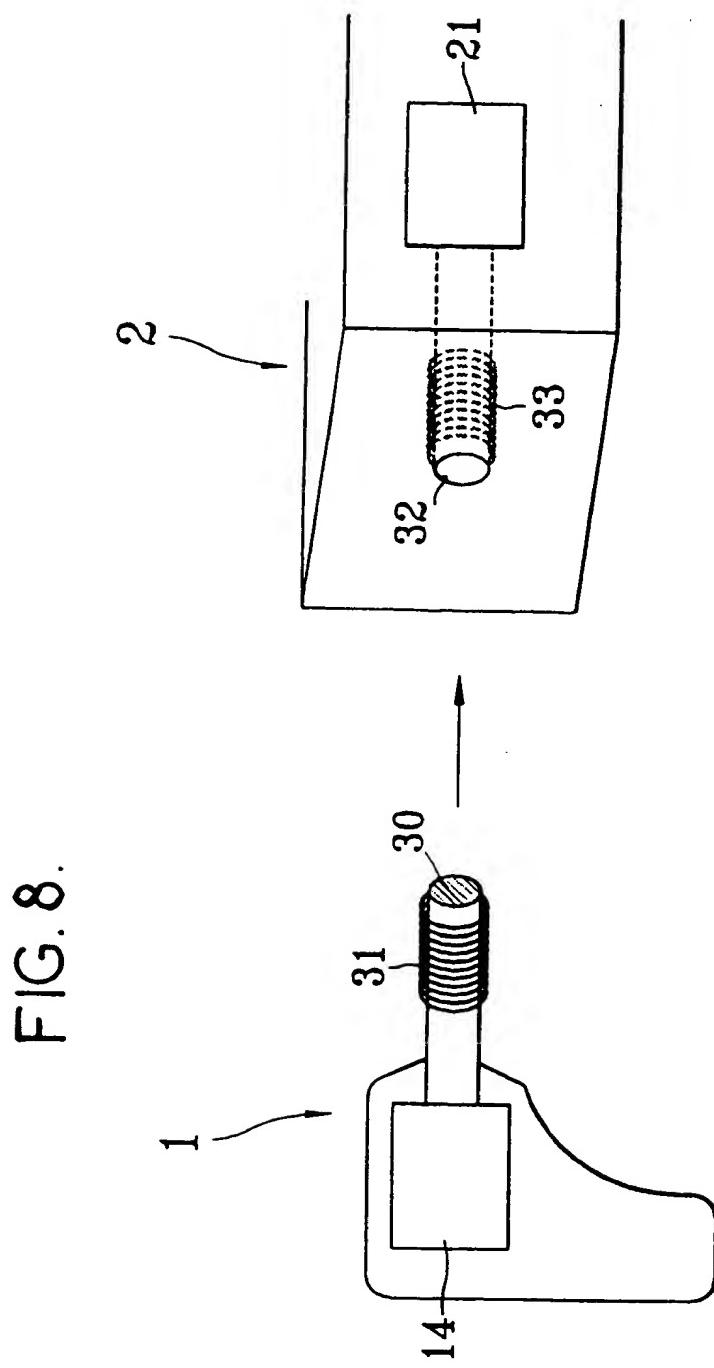


FIG. 7.



THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)